https://www.wealthmanagement.com/technology/growing-need-cyber-insurance

akinbostanci/iStock/Getty Images Plus

TECHNOLOGY

The Growing Need For Cyber Insurance

Digital fraud is a growing threat to advisors, who are on their own when it comes to buying coverage for the risk.

Rob Burgess | Aug 17, 2023

Chad Ramberg, who sells insurance to financial advisors, called it the "craziest claim" he worked on last year.

An advisor Ramberg works with met with a client in the advisor's office. The client told the advisor he had just purchased a house and needed help sending $300,000 to the real estate escrow company. The advisor made the arrangements to transfer the funds from the client's custodial account, then called to ensure the payment was received.

"I don't know what you're talking about," was the answer from the holder of the escrow account.

The client had fallen prey to a sophisticated social engineering scam. The fraudster had hacked into the client's email account and monitored it for notifications of any large transactions. When the real escrow company sent

the request for funds, the fraudster deleted the legitimate email and replaced it, inserting a fraudulent account number to receive the transfer.

The advisor notified the custodian and stopped the transfer.

A social engineering scam against a financial advisor and their client is a prime example why cybersecurity insurance is needed, Chad Ramberg says.

Had the money been lost, the advisor was covered by cyber fraud insurance, a relatively obscure—and in many cases completely optional—insurance policy for advisors that protects against losses from sophisticated digital fraud, data breaches or cybercrimes.

These policies are different than an advisor's typical E&O (errors and omissions) insurance, which largely covers inadvertent but costly advisor mistakes.

Demand for cyber insurance is growing, according to the U.S. Government Accountability Office. Insurance customers opting for cyber coverage jumped from 26% in 2016 to 47% in 2020, according to the agency. At the same time, the costs of cyberattacks nearly doubled, according to the GAO. With the rise of attacks, including those using generative AI, the risks to advisors, and their clients, grow daily.

Spotty Government Oversight

There are few legal requirements for advisors to carry any insurance at all, much less policies against cyber fraud. Standards are non-existent, risks are not fully understood even by policy writers, and premiums are all over the map.

Under the proposed SEC Cybersecurity Risk Management Rules, firms would need to have documented processes in place to mitigate and respond

to “significant cybersecurity incidents” and report them to the SEC when they happen—including whether any losses are covered by insurance policies, said Tiffany Magri, senior regulatory advisor at Smarsh, a compliance technology firm.

However, the commission’s proposal does not require cyber fraud insurance. According to one advisor, if the SEC made cyber fraud insurance a requirement, it would be an easier hurdle to clear than all the other requirements regulators demand. “A simple insurance requirement based on [the] amount of assets would solve this in a much simpler fashion,” by letting the market decide how much risk exists and how much protection an advisor needs, wrote an RIA compliance officer in a comment letter to the SEC.

Only three states mandate advisor E&O insurance, and only one of those specifically mention insurance against the risk of a cybersecurity breach.

Erika Safran, of Safran Wealth Advisors in New York City, with $100 million in AUM and two employees, carries E&O and cyber policies through Markel. She pays $4,800 annually.

In 2017, the Securities Division for the Vermont Department of Financial Regulation instituted a rule that advisors must have “adequate insurance” for such breaches. What “adequate” means depends on the firm’s size, organizational structure and the number and location of offices.

Also in 2017, the Oregon Legislative Assembly passed requirements for advisors there to purchase at least a $1 million errors and omissions (E&O) insurance policy, which may cover some, but not all, costs of a data breach.

“Once Oregon mandated it, I was expecting to see many states follow suit,” said Lilian A. Morvay, principal and founder of the Independent Broker Dealer Consortium, a cooperative organization that aggregates services for the IBD and RIA communities. “They have not.”

In 2020, Oklahoma also began requiring advisors to carry E&O insurance, but no mention or requirements that such policies cover cyber fraud.

Ramberg said the general lack of regulatory oversight in this area was a double-edged sword.

“The Texas in me doesn’t like the requirements because it paints everybody with a broad brush,” he said. But the lack of standards means many advisors who do opt for coverage can pay either too little or too much for their risks. Those with too little coverage would not be aware of the mismatch “until something happens, that’s the problem.”

Business Requirements Often Drive Adoption

While the state-by-state requirements are scattershot, advisors may find they won’t be able to do business unless they carry the insurance policies their custodians require—but even there, it’s unclear how much the mandated insurance covers losses to cyber fraud, versus traditional E&O insurance.

For example, Schwab requires advisors to carry an aggregate minimum of $1 million of insurance coverage to protect against E&O, as well as “social engineering” and “theft by hackers.”

Neither Fidelity nor Pershing would comment on the specific requirements for the advisors they work with.

The vendors may be reluctant to saddle their advisor clients with additional, and costly, requirements. Cyber fraud insurance covers risks that a traditional E&O policy may not, but can cost considerably more. Some advisors may choose instead to invest the additional resources in better cyber security.

While an E&O insurance policy may, in some cases, cover an advisor's professional liability in case of a cyberattack, many other associated costs incurred in the fallout—including ransoms, data restoration and lost profits from business interruption—would not.

Alvin Carlos, of District Capital Management in Washington, D.C., with $13.6 million in AUM and five employees, carries a $1 million E&O policy and $500,000 employment practices and liability insurance through The Hartford. He pays $4,100 annually ($2,500 for E&O with a $500 deductible; $1,600 for EPL)

Noel Paul, a partner at Reed Smith, a law firm that represents financial advisors and other commercial policyholders in negotiating and obtaining insurance coverage, said the cyber insurance landscape is "very fluid" as policies differ significantly from one insurance carrier to another.

A standalone cyber insurance policy offers the most comprehensive coverage, Paul said. An E&O policy would often only cover a liability claim in which an advisor was negligent in protecting a client's financial data.

William Trout, director of wealth management for Javelin Strategy and Research, said cyber insurance offers an extra layer of protection advisors may need given the growing complexity of their technology integrations and reliance on third-party vendors.

“The digital surface area has gotten so large that there are so many different points of attack,” he said.

The Independent Broker Dealer Consortium's Morvay said RIAs should work with insurance providers who have specific experience with advisors.

Traditional carriers like Chubb, AIG, The Hartford and Travelers will underwrite policies, as well as more specialized firms like At-Bay and Lloyd Beazley, but “cybersecurity policies are complicated, and no two policies are alike,” Morvay said.

Providers sometimes offer combined E&O and cyber insurance policies, but Paul said advisors should be wary of gaps in coverage. The policies often have a combined coverage limit, meaning a cyber claim would draw down on the policyholder’s limits for professional liability. Standalone cyber and E&O policies avoid that problem, he said.

Advisors should look for a cybersecurity policy that is “Pay On Behalf Of,” which ensures that the carrier will pay losses and expenses once the per-claim deductible has been satisfied, Morvay said. This contrasts with a “Reimbursement Policy,” which requires an RIA to seek reimbursement for covered losses and damages from the carrier, which could take weeks if not months.

Another important feature to look for in a cybersecurity policy, Morvay said, is coverage for “Post Breach Remediation Costs.” Some policies will limit the amount that is available for these expenses, while other carriers will cover them at no additional cost or deductible to the RIA.

Cyber insurance policies can even contain coverage for extortion costs from a ransomware attack, in which they will negotiate with the hackers and even pay the ransom itself. Insurance companies prefer to pay those costs on a cyber claim as opposed to the often more expensive alternative, which involves attempting to retrieve and restore data that might be encrypted or damaged, Paul said.

Harris Nydick, of CFS Investment Advisory Services in Totowa, N.J., with $2 billion in AUM and 14 full-time employees, carries separate E&O and cyber policies from The Twin City Fire Insurance Company at At-Bay. He pays about $36,000 annually.

But finding insurance providers to cover a ransomware attack specifically is challenging, despite it being one of the major areas of concern, said Sid Yenamandra, founder, CEO and managing partner at Surge Ventures.

“The problem is it’s like offering flood insurance in a high flood zone,” he said. “Everyone out there is susceptible to a ransomware attack. … Insurance vendors aren’t supporting it in many cases and ransomware is one of the biggest draws of insurance.”

Companies that do offer ransomware protection will only underwrite firms that have significant cyber security tools, and staffing, in place.

“To be on the right side of the loss ratio for you as an insurance provider you only want to take on certain risks,” he said. “You’ve got to weed them out. … It’s like a college application. It’s tough.”

Before a cybersecurity carrier writes a policy for an advisor, Morvay said the carrier will conduct an analysis of the firm and try to identify any cybersecurity risks. Some carriers will work with the firm to address the vulnerabilities of an insurance client for free. Once a policy is written, they may conduct periodic monitoring of the security during the policy period.

The reality is few know with certainty how much risk advisors, and their clients, have from cyber fraud, nor how much insurance is needed to cover them.

Unlike traditional underwriting that relies on actuarial science backed by many decades of historical data, the risks from cyber fraud are evolving.

“Past is not ... predictive of future,” Yenamandra said. “Underwriting models are in question at the moment.”